

UPGRADEABLE TIMESTAMP MECHANISM5 **1. Field of the Invention:**

 The present invention relates generally to digital
timestamps. Specifically, the present invention is
directed toward a digital timestamp that may be updated
to preserve its integrity as cryptographic technologies
10 become obsolete.

2. Background of the Invention:

 Digital time stamps, like their paper counterparts,
are used to certify that a specific document has not been
15 modified since a specific date. A digital time stamp
includes a hash value calculated from the document to be
time stamped, the current time at the time of the
timestamp, and a digital signature signing both the hash
value and the current time.

20 The digital signature and hash value are what make a
timestamp secure (i.e., they ensure the authenticity of
the timestamp). Digital signatures generally rely on
public key cryptosystems such as the Rivest-Shamir-
Adleman (RSA) public-key cryptosystem. Hash values are
25 calculated using hash functions such as SHA-1 (Secure
Hashing Algorithm 1) and MD5 (Message Digest 5), which
map entire documents into fixed-bitlength numbers. If
the integrity of either the hash function used to produce
the hash value or the cryptosystem used to produce the

Docket No. 2001-088-NSC

digital signature is compromised, the timestamp's integrity is ruined as well.

Many real-life applications of computer technology depend on the long-term storage of data. An example of this is the U.S. Internal Revenue Service's use of computers to store information regarding taxable gifts made over a person's lifetime. For most people living in the United States, gift taxes are not calculated or paid until death, so any information regarding taxable gifts must be maintained over a person's lifetime. In terms of probable advances in computer technology and cryptanalysis, a person's lifetime is like an eternity—it is impractical to assume that the cryptosystems available today will provide any measure of security in 50-70 years. Thus, a need exists for a timestamping mechanism that can adapt to changes in technology to provide a secure timestamp over a long duration of time.

SUMMARY OF THE INVENTION

The present invention provides a method, computer
program product, and data processing system for
5 generating and validating an upgradeable digital
timestamp of a document. The digital timestamp includes
a hash value, a current time, and a digital signature.
Over time, as computer and cryptanalytic technology
progresses, upgrade timestamps are applied to the
10 document that take advantage of more advanced, more
difficult to break hash functions or digital signature
schemes. These upgrade timestamps are applied
preventatively at a point in time just prior to the
timestamp's being able to be compromised.

BRIEF DESCRIPTION OF THE DRAWINGS

The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself, however, as well as a preferred mode of use, further objectives and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

Figure 1 is an external view of a computer system in which the present invention may be implemented;

Figure 2 is a block diagram of a computer system in which the present invention may be implemented;

Figure 3 is a diagram depicting a process of applying an upgradeable time stamp to a document in accordance with a preferred embodiment of the present invention;

Figure 4 is a diagram of a process of updating a time stamp to reflect a more powerful digital signature algorithm in accordance with preferred embodiment of the present invention;

Figure 5 is a diagram depicting a process of updating a time stamp to reflect a new hash function in accordance with a preferred embodiment of the present invention;

Figure 6 is a diagram depicting a process in a preferred embodiment of the present invention whereby a document is verified to have not been tampered since an initial time stamp was placed on the document; and

[illegible][illegible]

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference now to the figures and in particular
5 with reference to **Figure 1**, a pictorial representation of
a data processing system in which the present invention
may be implemented is depicted in accordance with a
preferred embodiment of the present invention. A
computer **100** is depicted which includes system unit **102**,
10 video display terminal **104**, keyboard **106**, storage devices
108, which may include floppy drives and other types of
permanent and removable storage media, and mouse **110**.
Additional input devices may be included with personal
computer **100**, such as, for example, a joystick, touchpad,
15 touch screen, trackball, microphone, and the like.
Computer **100** can be implemented using any suitable
computer, such as an IBM RS/6000 computer or
IntelliStation computer, which are products of
International Business Machines Corporation, located in
20 Armonk, New York. Although the depicted representation
shows a computer, other embodiments of the present
invention may be implemented in other types of data
processing systems, such as a network computer. Computer
100 also preferably includes a graphical user interface
25 (GUI) that may be implemented by means of systems
software residing in computer readable media in operation
within computer **100**.

With reference now to **Figure 2**, a block diagram of a
data processing system is shown in which the present
30 invention may be implemented. Data processing system **200**

Docket No. 2001-088-NSC

is an example of a computer, such as computer 100 in **Figure 1**, in which code or instructions implementing the processes of the present invention may be located. Data processing system 200 employs a peripheral component interconnect (PCI) local bus architecture. Although the depicted example employs a PCI bus, other bus architectures such as Accelerated Graphics Port (AGP) and Industry Standard Architecture (ISA) may be used. Processor 202 and main memory 204 are connected to PCI local bus 206 through PCI bridge 208. PCI bridge 208 also may include an integrated memory controller and cache memory for processor 202. Additional connections to PCI local bus 206 may be made through direct component interconnection or through add-in boards. In the depicted example, local area network (LAN) adapter 210, small computer system interface SCSI host bus adapter 212, and expansion bus interface 214 are connected to PCI local bus 206 by direct component connection. In contrast, audio adapter 216, graphics adapter 218, and audio/video adapter 219 are connected to PCI local bus 206 by add-in boards inserted into expansion slots. Expansion bus interface 214 provides a connection for a keyboard and mouse adapter 220, modem 222, and additional memory 224. SCSI host bus adapter 212 provides a connection for hard disk drive 226, tape drive 228, and CD-ROM drive 230. Typical PCI local bus implementations will support three or four PCI expansion slots or add-in connectors.

An operating system runs on processor 202 and is used to coordinate and provide control of various components within data processing system 200 in **Figure 2**. The

Docket No. 2001-088-NSC

operating system may be a commercially available operating system such as Windows 2000, which is available from Microsoft Corporation. An object oriented programming system such as Java may run in conjunction with the
5 operating system and provides calls to the operating system from Java programs or applications executing on data processing system 200. "Java" is a trademark of Sun Microsystems, Inc. Instructions for the operating system, the object-oriented programming system, and applications
10 or programs are located on storage devices, such as hard disk drive 226, and may be loaded into main memory 204 for execution by processor 202.

Those of ordinary skill in the art will appreciate that the hardware in **Figure 2** may vary depending on the
15 implementation. Other internal hardware or peripheral devices, such as flash ROM (or equivalent nonvolatile memory) or optical disk drives and the like, may be used in addition to or in place of the hardware depicted in **Figure 2**. Also, the processes of the present invention
20 may be applied to a multiprocessor data processing system.

For example, data processing system 200, if
optionally configured as a network computer, may not include SCSI host bus adapter 212, hard disk drive 226,
25 tape drive 228, and CD-ROM 230. In that case, the computer, to be properly called a client computer, must include some type of network communication interface, such as LAN adapter 210, modem 222, or the like. As another example, data processing system 200 may be a
30 stand-alone system configured to be bootable without

Docket No. 2001-088-NSC

relying on some type of network communication interface, whether or not data processing system 200 comprises some type of network communication interface. As a further example, data processing system 200 may be a personal digital assistant (PDA), which is configured with ROM and/or flash ROM to provide non-volatile memory for storing operating system files and/or user-generated data.

The depicted example in **Figure 2** and above-described examples are not meant to imply architectural limitations. For example, data processing system 200 also may be a notebook computer or hand held computer in addition to taking the form of a PDA. Data processing system 200 also may be a kiosk or a Web appliance.

The processes of the present invention are performed by processor 202 using computer implemented instructions, which may be located in a memory such as, for example, main memory 204, memory 224, or in one or more peripheral devices 226-230.

Figure 3 is a diagram depicting a process of applying an upgradeable time stamp to a document in accordance with a preferred embodiment of the present invention. The document (D) 300 is encoded using a hash function 301 to produce hash value 302. A hash function is a function that maps an input of arbitrary finite bit length to an output of fixed bit length. Hash functions are typically used to detect data tampering. Some examples of hash functions existing in the art are the Secure Hash algorithm (SHA), the Message Digest algorithms including MD4 and MD5, the Matyas-Myer-Oseas

Docket No. 2001-088-NSC

algorithm, and the like. As the present invention allows the hash function to be updated, many different hash functions may be used without departing from the scope and spirit of the invention.

5 A real time clock 304 is used to produce a time value t 306. Time value t 306 is combined with hash value 302 to produce an ordered pair 308. (Note that while an ordered pair is depicted, the order in which the elements of the pair appear is immaterial to the operation of the present invention.) A digital signature algorithm 309 is then applied to ordered pair 308 to produce digital signature 310. A digital signature is a sequence of bytes that is dependent on some secret known by the creator of the digital signature and also dependent upon the message being signed. A secret is simply an amount of data that is known only to a select one or more parties. A digital signature serves to authenticate that a document, or other piece of data, was produced by a proper party, since only the proper party will know the correct secret with which to create an authentic signature. Some examples of existing digital signature schemes in the art include the Rivest-Shamir-Adleman digital signature scheme, the Fiat-Shamir signature scheme, and the Digital Signature Algorithm (DSA). As the present invention allows for the upgrading of digital signature algorithms, many different digital signature algorithms may be used in the present invention, including algorithms that have not yet been developed. To complete the time stamp, ordered pair 308 is combined with digital signature 310 to produce time stamp 312.

At this point, it is helpful to consider the significances of the information contained in time stamp 312. Time stamp 312 contains the time t at which the time stamp was created. Time stamp 312 also contains a hash value for document 300 at time t . This hash value can be compared with a computer hash value for document 300 to determine if document 300 has been modified since time t . Finally, time stamp 312 is signed with a digital signature. This means that the time stamp data, the time value t and the hash value, came from an authentic source. In other words, time stamp 312 was not forged.

At some point the underlying cryptographic technology supporting digital signature algorithm 309 may lose its effectiveness. As advances are made in computer technology and encrypt analysis, cryptographic schemes such as digital signature algorithm 309 will become easy to break.

Figure 4 is a diagram of a process of updating a time stamp to reflect a more powerful digital signature algorithm in accordance with preferred embodiment of the present invention. Preferably, the process depicted in **Figure 4** will be applied at some point not long before the digital signature algorithm used in the time stamp becomes susceptible to attack (i.e., is no longer secure). A previously created time stamp 312 is encoded using hash function 301 to produce a new hash value 402. Meanwhile, real time clock 304 is used to produce a new time value t' 406. Hash value 402 and time value t' 406 are combined to produce ordered pair 408. Ordered pair 408 is then processed using an updated digital signature

Docket No. 2001-088-NSC

algorithm 409 to produce digital signature 410. Finally, ordered pair 408 and digital signature 410 are combined to produce a new time stamp 412 to be recorded along with existing time stamp 312.

5 A similar process can be used to update a time stamp in the event that the hash function becomes obsolete.

Figure 5 is a diagram depicting a process of updating a time stamp to reflect a new hash function in accordance with a preferred embodiment of the present invention. As

10 with the process in Figure 4, the process depicted in Figure 5 will be applied preferably at some point not long before the hash function used in the time stamp loses its effectiveness. Unlike the situation in Figure 4, however, the old time stamp 312 is not used to

15 calculate the new time stamp 512. Instead, document 300 is directly encoded using a new hash function 501 to produce hash value 502. Real time clock 304 is used to produce time value t' 506. Hash value 502 and time value t' 506 are combined to produce ordered pair 508, which is
20 then signed using digital signature algorithm 309 to produce digital signature 510. Finally, ordered pair 508 and digital signature 510 are combined to produce a new time stamp 512 to be recorded along with existing timestamp 312.

25 Figure 6 is a diagram depicting a process in a preferred embodiment of the present invention whereby a document is verified to have not been tampered since an initial time stamp was placed on the document. Figure 6 deals with the situation in which the digital signature
30 algorithm was updated. Figure 7 deals with the

Docket No. 2001-088-NSC

alternative situation in which the hash function was updated.

Turning now to **Figure 6**, ordered pair **602** of the new time stamp is checked against digital signature **604** from the new time stamp to see if they correspond (stamp **600**). If they match, then the new time stamp has not been tampered with (**606**). Next, digital signature **610** of the original time stamp is checked against hash value **612** contained in ordered pair **602** of the new time stamp. If the computed hash value of digital signature **610** is identical to hash value **612** (step **608**), then digital signature **610** has not been modified since the time of the new time stamp (**614**).

Now ordered pair **618** of the original time stamp is used to verify digital signature **610** from the original time stamp. If they correspond (step **616**), then the original time stamp has not been tampered with (**620**). Finally, the document itself (**624**) is checked against hash **626** contained in ordered pairs **618** of the original time stamp (step **622**). If they match, then the document is good (**628**). In other words, document **624** has not been modified since the time of the original time stamp.

Figure 7 is a diagram depicting a process of verifying an updated time stamp where a hash function has been updated, in accordance with a preferred embodiment of the present invention. First, ordered pair **702** and digital signature **704** from the updated time stamp are compared (step **700**). If they correspond, then it is known that the document has not been tampered with since the time of the updated time stamp (**706**). Finally,

Docket No. 2001-088-NSC

ordered pair 710 and digital signature 712 from the original time stamp are compared (step 708). If they correspond, then the document has not been tampered with since the time of the original time stamp (714) (since we
5 know that the timestamp was not tampered with between the time of the original and updated time stamps, and we know from validating the second time stamp that the second timestamp has not been tampered with).

It is important to note that while the present
10 invention has been described in the context of a fully functioning data processing system, those of ordinary skill in the art will appreciate that the processes of the present invention are capable of being distributed in the form of a computer readable medium containing
15 instructions or other functional descriptive data in various forms. The present invention is equally applicable, regardless of the particular type of signal bearing media actually used to carry out the distribution. Examples of computer readable media
20 include recordable-type media such a floppy disc, a hard disk drive, a RAM, CD-ROMs, magnetic tape, and transmission-type media such as digital and analog communications links.

The description of the present invention has been
25 presented for purposes of illustration and description, and is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art. The embodiment was chosen and described in
30 order to best explain the principles of the invention,

[illegible]

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
0	0.0000	0.0001	0.0002	0.0003	0.0004	0.0005	0.0006	0.0007	0.0008	0.0009	0.0010	0.0011	0.0012	0.0013	0.0014	0.0015	0.0016	0.0017	0.0018	0.0019	0.0020	0.0021	0.0022	0.0023	0.0024	0.0025	0.0026	0.0027	0.0028	0.0029	0.0030	0.0031	0.0032	0.0033	0.0034	0.0035	0.0036	0.0037	0.0038	0.0039	0.0040	0.0041	0.0042	0.0043	0.0044	0.0045	0.0046	0.0047	0.0048	0.0049	0.0050	0.0051	0.0052	0.0053	0.0054	0.0055	0.0056	0.0057	0.0058	0.0059	0.0060	0.0061	0.0062	0.0063	0.0064	0.0065	0.0066	0.0067	0.0068	0.0069	0.0070	0.0071	0.0072	0.0073	0.0074	0.0075	0.0076	0.0077	0.0078	0.0079	0.0080	0.0081	0.0082	0.0083	0.0084	0.0085	0.0086	0.0087	0.0088	0.0089	0.0090	0.0091	0.0092	0.0093	0.0094	0.0095	0.0096	0.0097	0.0098	0.0099	0.0100